

# Live Forensics Analysis Method For Random Access Memory On Laptop Devices

<sup>1</sup>Danang Sri Yudhistira, <sup>2</sup>Imam Riadi, <sup>3</sup>Yudi Prayudi

<sup>1</sup>Department of Informatics, Universitas Islam Indonesia

<sup>2</sup>Department of Information System, Universitas Ahmad Dahlan

<sup>3</sup>Department of Informatics, Universitas Islam Indonesia

Email: <sup>1</sup>danangsriyudhistira@gmail.com, <sup>2</sup>imam.riadi@is.uad.ac.id, <sup>3</sup>prayudi@uii.ac.id

**Abstract**— The development of computer technology now have an impact on the increasing cases of cybercrime crime that occurred either directly or indirectly. Cases of cybercrime now are able to steal digital information is sensitive and confidential. Such information may include email, user\_id, and password. In addition to browser cookies stored on your computer or laptop hard drive, user\_id, email, and password are also stored in random access memory (RAM). Random access memory (RAM) is volatile so that in doing the analysis required an appropriate and effective method. Digital data acquisition method in random access memory can be done live forensics or when the system is running. This is done because if the device or laptop computer is dead or shutdown then the information stored in random access memory will be lost. In this study has successfully carried out its acquisition of random access memory (RAM) for information access rights and password login form user\_id on your websites such as Facebook, PayPal, internet banking, and bitcoin. Tools used to perform data acquisition, namely Linux Memory Extractor (LiME) and FTK Imager.

Keywords: Live forensics, RAM, laptop, devices.

## I. INTRODUCTION

Along with the increasing use of computer crimes, then the chance of cybercrime is also increasing. Cybercrime is not only done to cripple a network server but also with steal critical data from an individual, organization or business entity [1]. Cases of cybercrime are happening now has already led to the theft of user\_id or username, email, and password which is the nature of the personal information privacy for some people. Such information includes concerns about the facebook account, internet banking, PayPal, and bitcoin. User\_id and password could be abused by people not responsible for how to steal other people's property and accounts result can harm the legitimate owner of the account [2]. In addition the result of theft and user\_id password, could only occur if the label is a social media account stolen, whereas if the internet banking account is stolen then the possible occurred the crime of theft money transfer via internet banking to another account or by means of the imposition of a fee to the owner of the legitimate account if that account is used for illegal transactions with on behalf of the owner of legitimate internet banking account, however the address shipments addressed to the address of the thief [3].

Information in the form of email, user\_id, and password in addition to browser cookies stored on is also stored in random

access memory on a laptop device that we use to do the login permissions. For it takes a proper method or technique, in order to perform the analysis of the random access memory on a laptop device. This is because the data in random access memory is volatile in nature. Volatile data will be lost if the computer is turned off or having to restart. Acquisition of random access memory to get information of digital evidence can only be done when the system is running or running [4].

Volatile data stored in random access memory describes the whole activity is taking place on a computer system that is being used. Handling data in random access memory has to be careful because in addition to its data can be lost if the system is turned off, the use of the tools will leave a footprint that can potentially overwrite existing valuable evidence is in the random access memory. It is, therefore, necessary the proper method for monetizing digital evidence stored in random access memory. The data acquisition method using the method live forensics [5].

Live forensics methods aimed at handling incidents faster, more assured data integrity, encrypted data can be opened and allow the memory capacity is lower when compared to traditional forensic methods. The stages are done in performing data analysis on random access memory with the live forensics method i.e., collect, examine, analyze and report [6][7].

## II. LITERATURE REVIEW

In research conducted by (Anand, 2016) explained that the random access memory storing log-related information activities carried out by the user and the system is running [8].

Previous research conducted by (Nisbet, 2016) data acquisition device is done on a laptop is usually just for the acquired data information that exists on the hard disk but this time it could be done for the acquired data in random access memory. The focus of this study is to acquire data in random access memory to find files that are encrypted [9].

In research conducted by (Stüttgen, Vömel, & Denzel, 2015) explained that results from acquisitions in the random access memory we can see potential malware attacks. In addition, we can recognize malicious programs that are already installed on a computer operating system [10].

Research in methods of live forensics to analyze the random access memory requires accuracy in finding existing digital evidence. There is some hitch in the study of random access memory. For ease of handling the method live forensics as well as keeping the value of the integrity of the evidence, it will be accessible with the python scripting language (Bharath & R, 2015) [11].

Other research and development became the basis for the research is research conducted by (Divyang Rahevar, 2013). On the research tells us that hidden file-related information, user\_id, password, rootkits, and sockets are not only stored on the hard disk but also stored in random access memory [12].

In research conducted by (Richard Carbone, 2012), conducted 2 tools namely LiME and Fmem comparison to get results in the acquisition random access memory on the pc-based Linux operating system by using the framework volatility memory analysis [13].

Other research conducted by (Karayianni & Katos, 2012) and investigations about data privacy regarding the information which is personal data. The information in the form of passwords stored in random access memory. Process analysis of the random access memory when the computer is done in conditions of operation or running because if the computers in a dead condition then data stored in random access memory will disappear [14].

### III. CURRENT PRACTICES

#### A. Linux Memory Extractor (LiME)

Linux Memory Extractor (LiME) tapes loadable kernel module that is can be used to perform the acquisition of volatile memory on Linux based-powered device. To be able to use the LiME needed privilege as root. LiME is the first tools capable of capture random access memory as a whole [15].

#### B. FTK Imager

FTK Imager or complete language is "Forensic Toolkit Imager" is a stand-alone application for the hosts Access disk imaging Data. Access to Data is a company engaged in the field of digital forensics and provides solutions from a classroom stand-alone to enterprise-class for digital investigation process. FTK Imager tools are used to analyze the results of the data acquisition of the laptop-based Linux operating system [16].

### IV. ACQUISITION OF RANDOM ACCESS MEMORY

The source of data used for digital evidence in this study comes from the random access memory on the laptop-based Linux operating system. In making acquisitions in the random access memory there are several stages that are done as in figure 1.

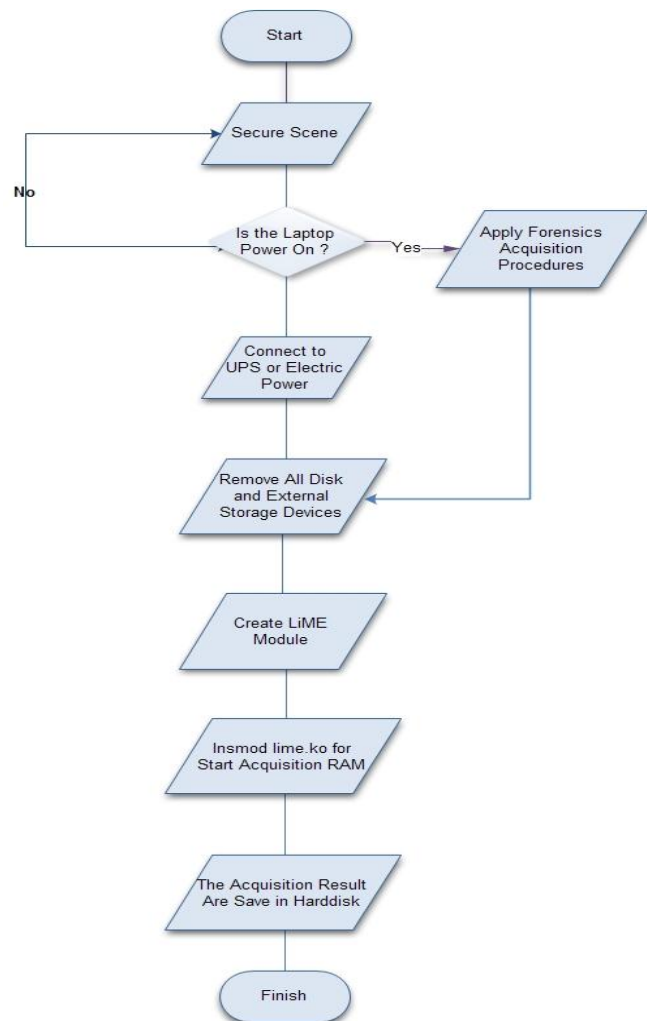


Figure 1. Flowchart Aqisition Of Random Access Memory

In Figure 1 that the first process begins with securing the scene of things. If the laptop is turned on then it can be done the next process, namely the acquisition of random access memory. Do not ever take off the power cable so that the laptop did not die when it conducted the process data acquisition. Prior to the acquisition process begins, remove all external storage that is stuck to the laptop. Create module LiME (Linux Memory Extractor) and type the command instead to begin the process of capture random access memory. Proceeds from the sale to random access memory will be stored automatically in the folder directory/home.

To create the LiME module (Linux Memory Extractor) first we go to the directory/src on the LiME-master folder located in folder Download by typing commands in accordance with Figure 2.

```
root@lepiku:/home/santoku/Downloads# cd LiME-master
root@lepiku:/home/santoku/Downloads/LiME-master# ls
doc LICENSE README.md src
root@lepiku:/home/santoku/Downloads/LiME-master# cd src
root@lepiku:/home/santoku/Downloads/LiME-master/src# ls
disk.c          lime.h          lime.o          Makefile        Module.symvers
disk.o          lime.mod.c      main.c          Makefile.sample tcp.c
lime-4.4.0-31-generic.ko lime.mod.o      main.o          modules.order   tcp.o
```

Figure 2. Access of LiME On The Directory SRC

Figure 2 describes the process to access the Linux Memory module Extractor (LiME) on the Linux operating system-based laptop. The process is done in a live forensics or laptop in the condition turned on.

The next process to capture the memory on a random access memory by typing commands at the command line terminal Linux fits in Figure 3

```
root@lepiku:/home/santoku/Downloads/LiME-master/src# insmod lime-4.4.0-31-generic.ko "path=/home/santoku/skenario-linux.lime format=lime"
root@lepiku:/home/santoku/Downloads/LiME-master/src#
```

Figure 3. Order to Capture Of Random Access Memory

Figure 3 describes the process of capture random access memory on Linux laptop device. Capture process starts with access to the directory/SRC to find the kernel module lime-4.4.0-31-generic. ko. Next, do the process of capture by typing commands at the command line Linux terminal according to Figure 3. Proceeds from the sale to random access memory on the laptop-based Linux operating system will be stored in the directory/home.

Proceeds from the sale to random access memory there is a file with the extension \*. lime. This file can be analyzed using tools FTK Imager that runs the Windows operating system. Analysis of the results obtained some information that can be used as evidence. Such information concerns the user\_id and password that originates from the internet banking account, PayPal, Bitcoin, and Facebook.

## V. THE ANALYSIS OF RANDOM ACCESS MEMORY

Based on the results of the acquisition of the random access memory on the laptop-based Linux operating system there is some related information that can be used as evidence. The information of which is information that is confidential or privacy because it is a personal account belonging to someone who used to do the login permissions an application on the website.

In this research have successfully found evidence in the form of digital information user\_id and password used to access the internet banking login, PayPal, Bitcoin and facebook. The information clearly captured by tools Linux Memory Extractor (LiME) and able to be analyzed using tools FTK Imager.

The first successful evidence obtained is the user\_id and password to access login to facebook website page. Proof of this is in addition to stored in browser cookies are also stored in random access memory devices. Evidence of the user\_id and password facebook listed in Figure 4.

14	01	AD	14	01	01	68	74-74	70	73	3A	2F	2F	77	77		https://ww
7E	2E	66	61	63	65	62	6F-6F	6B	2E	63	6F	6D	2F	6C		w.facebook.com/l
6F	67	69	6E	2E	70		70-68	74	74	70	73	3A	2F	6F		login.php?http=
77	6C	77	2E	66	61	63	65-62	6F	6B	2E	63	6F	6D	2F		www.facebook.co
2F	6C	77	67	69	6E	2E	70-68	70	65	6D	61	69	6C	6F		/login.phpemailid
61	6E	74	79	75	64	68	69-73	74	69	72	61	40	72	6F		kanyudhistira@o
63	65	74	74	6D	61	69	6C-2E	63	6F	6D	70	61	73	78		cketmail.compass
6A	F6	6A	77	71	32	63	66-61	63	65	62	6F	6B	7B	78		jaglal2371@tups
63	6F	6D	2F	01	61	6A	64-C4	DF	00	00	00	00	00	00		facebook.
00	00	40	0B	00	00	E1	00-00	00	0A	00	00	00	C2	00		.com...ZdAs
6F	00	67	00	69	00	06	00-SF	00	66	00	6F	00	72	00		-g-o-i-n_-f-o-r-
6D	00	40	00	00	00	70	00-6F	00	73	00	04	01	C6	06		m....p-o-s-t-A-
00	00	68	74	74	70	73	3A-2F	2F	77	77	2E	66	61			..https://www.fa
63	65	62	6F	6B	2E	63	63-6F	6D	2F	6C	6F	67	69	6E		cbook.com/login
2E	70	68	70	3F	73	6B	69-70	5F	61	70	69	5F	6C	6F		.php?skip api io

Figure 4. Evidence Of The Facebook Account

Based on the analysis of the results of the acquisition of random access memory that is listed in Figure 4, note that proof of access logs in facebook using the email account "danzyudhistira@rocketmail.com" and the password "jogja123571". This evidence will still be stored in random access memory and will not be lost as long as the laptop is not turned off.

Other evidence that successfully obtained i.e. access login to your website belongs to national banking. Access to internet banking transaction. Evidence from access the login listed in Figure 5.

[illegible]

### Figure 5. Evidence Of The Internet Banking Account

Based on the analysis of the results of the acquisition of random access memory that is listed in Figure 5, it is noted that proof of access to the internet banking account login using user \_ id "danangsr1911" and the password "123571". The account is stored in random access memory without experiencing encryption. This proves that the internet banking application belongs to the national banking still vulnerable to acts of theft user\_id and password by the person who is not liable if it managed to get the account access login.

In addition, there is evidence of the access account login bitcoin. Bitcoin is a cryptocurrency currency now is quite popular to use for online transactions. Bitcoin account login access evidence listed in Figure 6.

[illegible]

Figure 6. Evidence Of The Bitcoin Account

Based on the analysis of the results of the acquisition of the random access memory on a laptop device as listed in Figure 6, note that the proof of the access account login using bitcoin email "danangriyudhistira@gmail.com" and the password "Yogyakarta123571". Just as the internet banking account, the account is also not experiencing bitcoin encryption.

Other evidence of the successful results obtained from sale to random access memory on the device operating system Linux-based laptop that is PayPal account login access. A PayPal account is also often used for payment transactions online. PayPal applies internationally making it easy to use just about any transaction. Paypal account login access evidence listed in Figure 7.

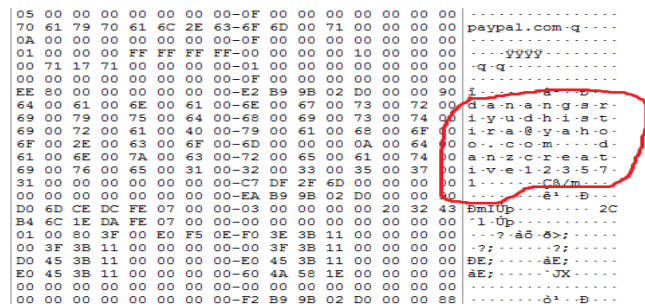


Figure 7. Evidence Of The Paypal Account

Based on the analysis of the results of the acquisition of the random access memory on a laptop device as listed in Figure 7, note that evidence access login your Paypal account using the email "danangsriyudhistira@yahoo.com" and the password "danzcreative123571". This evidence will still be stored in random access memory for laptop device is not turned off. Just as the internet banking accounts and user\_id and password bitcoin, PayPal account stored in random access memory is also not experiencing the encryption

## VI. CONCLUSION

After a series of research and analysis of random access memory on the device, a laptop with Linux operating system using the method live forensics can be drawn the conclusion that random access memory capable of storing all the information all the related activities performed by the user or users. In this case, it is activities to access internet banking login, PayPal, Bitcoin, and Facebook. Proof of access the login i.e. user\_id and password. Tools Linux Memory Extractor (LiME) able to do capture memory thoroughly so that the information obtained from random access memory was able to complete and can be used as evidence in a digital handling of crimes and involve evidence-based laptop Linux operating systems. While the FTK Imager tools are able to perform analysis of digital evidence properly because of evidence that encrypted not encrypted are also capable opened by these tools.

## VII. FUTURE WORK

This research has managed to find a social media account login access facebook, internet banking, bitcoin and PayPal stored in random access memory on the device a laptop either user\_id or username and password. For the development of further research is expected to find a credit card account that was inputted when we conduct E-Commerce transactions to shop online using a browser laptop. In addition to the credit card account is saved in the browser's cookies will also be

stored in random access memory on a device that is used for the transaction, in this case, using a laptop devices

## REFERENCES

- [1] Wahyudi, E., Indonesia, U. I., Riadi, I., Dahlan, U. A., Pray, Y., & Indonesia, U. I. (2018). Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence. *International Journal of Computer Science and Information Security (IJCSIS)*, 16(2), 1–7.
- [2] Prayogo, A., Riadi, I., & Luthfi, A. (2017). Mobile Forensics Development of Mobile Banking Application using Static Forensic. *International Journal of Computer Applications*, 160(1), 5–10.
- [3] Riadi, I., & Umar, R. (2017). Identification Of Digital Evidence On Android 's. *International Journal of Computer Science and Information Security*, 15(5), 3–8.
- [4] Dave, R., Mistry, N. R., & Dahiya, M. S. (2014). Volatile Memory Based Forensic Artifacts & Analysis. *International Journal For Research In Applied Science and Engineering Technology*, 2(I), 120–124.
- [5] Rochmadi, T., Riadi, I., & Prayudi, Y. (2017). Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser. *International Journal of Computer Applications (IJCA)*, 164(8), 31–37.
- [6] Riadi, I., Eko, J., Ashari, A., & -, S. (2013). Internet Forensics Framework Based-on Clustering. *International Journal of Advanced Computer Science and Applications*, 4(12), 115–123.
- [7] Umar, R., Riadi, I., & Zamroni, G. maulana. (2017). A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements. *International Journal of Advanced Computer Science and Applications*, 8(12), 69–75.
- [8] Anand, V. N. (2016). Acquisition Of Volatile Data From Linux System. *International Journal of Advanced Research Trends in Engineering and Technology*, 3(5), 95–97.
- [9] Nisbet, A. (2016). Memory forensic data recovery utilising RAM cooling methods, 11–16.
- [10] Stüttgen, J., Vömel, S., & Denzel, M. (2015). Acquisition and analysis of compromised firmware using memory forensics. *DFRWS 2015 Europe*, 12(S1), S50–S60.
- [11] Bharath, B., & R, N. M. A. (2015). Automated Live Forensics Analysis for Volatile Data Acquisition. *Int. Journal of Engineering Research and Applications*, 5(3), 81–84.
- [12] Divyang Rahevar. (2013). Study on Live analysis of Windows Physical Memory. *IOSR Journal of Computer*



*Engineering (IOSR-JCE)* , 15(4), 76–80.

- [13] Richard Carbone. (2012). The definitive guide to Linux-based live memory acquisition tools. *DRDC Valcartier TM 2012-319*.
- [14] Karayianni, S., & Katos, V. (2012). Practical password harvesting from volatile memory. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, 99 LNICST(May 2014), 17–22.
- [15] LiME, <https://github.com/504ensicsLabs/LiME>, 2018
- [16] FTK Imager, <https://accessdata.com>, 2018